# Cyber Security in API Economy – Issues & Challenges

**Conference Paper** · March 2016



Lakshmi Shankar Iyer
Christ University, Bangalore

# Cyber Security in API Economy – Issues and Challenges

**Lakshmi Iyer**
Institute of Management, Christ University
Bengaluru, India
**Email Id:** lakshmi.iyer@christuniversity.in

**Sirish Venkatagiri**
Institute of Management, Christ University
Bengaluru, India
**Email Id:** sirish.venkatagiri@christuniversity.in

***Abstract – Application programming interfaces – APIs as they are called - have a long history, and started to gain prominence when Operating Systems such as Microsoft Windows started to build their ecosystem (they came as part of the Software Development Kit or SDK, and were called Windows APIs). Essentially, APIs expose the services provided by the software they are built upon to the other organizations that wish to extend their functionality. For example, before Microsoft Windows incorporated device drivers for most printers, hardware manufacturers had to write the device drivers for their printers using the APIs provided along with the Operating System. Since then, APIs have increasingly become important in the Digital ecosystem, to the extent that the term "API economy" has come to be framed. One leading example of an API set that has gained momentum and is a part of GE's Industrial Internet, is called Predix.***

***GE notched up a turnover of $1 billion from its Industrial Internet initiative in 2015. GE's Predix is being deployed in a variety of industrial environments, all across the various sectors in which GE has a presence. Some of them are: avionics, transportation, and energy. According to Gartner, 75% of the Fortune 1000 companies will provide APIs within the next few years. Indeed, Salesforce.com admitted that a certain percentage of their revenue could be attributed to their partnerships through the medium of API's. In India too, UIADI's Aadhaar provided APIs to benefit organizations that could leverage the huge amount of data that is being collected on the citizenry.***

***As APIs continue to occupy centre stage in the increasingly Digital world, the cyber security aspect looms large on the horizon. This is especially so in contexts where the Digital meets the physical world e.g. in avionics. The Stuxnet incident (Iran's nuclear reactor coming under cyberattack through malware, reference) is a salient example. Privacy too, is a concern.***

***To date, GE's Predix is in Beta, being made available to a small number of partners before its commercial release.***

***In India, the Aadhaar ecosystem based on Unique Identification Authority of India's (UIDAI) Aadhaar APIs is in its infancy. The former CTO of Aadhaar, Shrikanth Nadhamuni, is now Founder of Khosla Labs, and the CEO of Novopay, which relies on Aadhaar APIs for authentication. Khosla Labs intends to devote attention to Aadhaar Applications, and has one more company, Aadhaar Bridge under its patronage. Khosla Labs conducted an Aadhaar Hackathon in 2015 in partnership with NASSCOM, where over 5000 developers participated. Soon after the Khosla Labs hackathon, another company, AngelPrime conducted another Aadhaar Hackathon, also in partnership with NASSCOM. What is of concern, from a cyber security and privacy perspective though, is that initially it was said that the APIs would only provide a "Yes/No" output to those using their APIs, but now a lot more data – such as Name of the Aadhaar holder, Age, Date of birth - is going to be made available.***

***Keywords – Aadhaar, API, API economy, Cyber security, Industrial Internet, Internet of Things, Predix.***

NOMENCLATURE

API – Application Program Interface – provision of access to external or internal software/systems by a software
ATM – Automated Teller Machine
C2M2 – Cyber security Capability Maturity Model – a model developed to assess the cyber security of a given organization
CEO – Chief Executive Officer
CTO – Chief Technology Officer
eKYC – electronic Know Your Customer – details provided by Aadhaar in response to an API request for customer details
GE – General Electric – the century old industrial conglomerate that provides products and services in several sectors internationally.
IoT – Internet of Things – Extensive use of sensors for collection of data typically in a consumer environment such as a car or in the industrial environment e.g. aircraft.
IIoT – Industrial Internet of Things – GE's term for the Internet of Things deployed in an industrial context. For example use of sensors on aircrafts to assess fuel efficiency based on big data acquired during a flight.

NASSCOM – National Association of Software and Services Companies – flagship of the Indian Information Technology and Information Technology enabled Services companies.
NCSP 2013 – National Cyber Security Policy – the Policy announced in 2013 relating to certain sections of IT Act 2000
OTP – one time pin

SDK – Software Development Kit – A collection of APIs provided by an organization to its partners for the development of its ecosystem.
SMS – Short Message Service

## I. INTRODUCTION

Application Programming Interface (API) may be thought of as a wrapper around an atomic functionality provided by the system for which it is made available. The system in consideration may even be a Legacy application, which cannot be modified to provide this service. APIs are most often provided in a Software Development Kit (SDK).
UIDAI has made available a set of APIs for Aadhaar. For example, one of the Aadhaar APIs provides Authentication services. A Bank that uses the Aadhaar API may programmatically send the Aadhaar Id of their new customer to UIDAI to ensure that the Aadhaar ID provided by their customer is valid. Based on the confirmation from UIDAI that this person exists and the Aadhaar ID provided by them belongs to them, the Bank can continue their Know Your Customer process. Initial applications of Aadhaar have been in the area of direct benefits transfer to citizens using their Aadhaar ID number.

While Aadhaar is in the Government domain, GE's Predix is a front runner in the Industrial domain. GE has coined several terms to emphasize the uniqueness of its offerings. The term Predix stems from Predictive. Due to GE being in several industry sectors such as Aviation, Energy, Transportation, Predix will be made available for the "Assets" (equipment) in these sectors gradually. Sensors are embedded in these Assets, and Predix is used as the interface between the Assets and the system/software application in which the Predix API calls are embedded. GE has talked about situations in which over $200,000 in potential repairs due to breakdown maintenance were avoided thanks to these sensors and Predix [1].
GE terms the new environment around Predix the Industrial Internet, to distinguish between the commercial Internet wherein the e-commerce companies abound, and the industrial Assets, where there is limited penetration of the Internet. The dawn of the new era in Industry with the Industrial Internet and Industrial Internet of Things (IIoT) is termed Industry 4.0.
APIs may be "Open" in the sense that they are documented and made available to other organizations. The Aadhaar API and GE's Predix are examples of Open APIs. It is hoped that the Open APIs will spawn an entire ecosystem. For example, the Aadhaar ID is just a 12-digit number. Only by the development of services and applications around it will the value of the ID increase, and the ID itself becomes meaningful [2]. Open APIs are also called Public APIs. Private APIs are APIs created for internal use only. Often, organizations create APIs for internal use, and after diligent testing may release some of them to the public, thereby making them "Open".

According to Gartner, 75% of the Fortune 1000 companies will offer Web APIs by 2016. Organizations have realized the commercial potential of providing APIs for their information, and are now eager to come up with a "Platform" strategy. For example, Microsoft Windows may be thought of as a Platform. Applications developed on top of Microsoft Windows have made the operating system popular, and difficult to displace from its pole position.

The proliferation of APIs has resulted in what may be termed the "API economy". GE recently reported that they achieved a turnover of $5 billion from their Industrial Internet (Predix) offering [3].

The same proliferation, while providing a Services avenue for revenue to the Industry behemoths, has a downside though. And this is the Cyber security aspect. The Heritage Foundation's Issue Brief of October 2014 lists month by month cyber attacks during the year [4]. Judging by this Brief alone, the cyber security situation is indeed alarming, even discounting the fact that the reported cyber attacks may only be a fraction of the total number of cyber attacks perpetrated during the given period. Even with Microsoft Windows (which was introduced in the 1980s), there were what were called "undocumented calls (i.e. APIs)". Some of the undocumented calls became common knowledge as contract employees switched jobs or current employees set up their own startups. Such a scenario could result in severe damages in the industrial environment. One example is that of the Stuxnet virus halting a uranium enrichment facility in Iran [5]. This is said to be the act of a State. Another example is that of a blast furnace in Germany, which had a breakdown due to hackers programmatically accessing its control system [6].

For both Aadhaar and Predix, which are Open APIs, cyber security is a major concern due to their intention to become ubiquitous. In the case of Aadhaar, the issue is one of citizen privacy being lost due to hacking, or worse. For Predix, the consequences can be dire, as it directly relates to industrial assets which may be interconnected and result in loss of human lives e.g. a locomotive or airplane going haywire, and failure of entire infrastructure e.g. electricity.
Keeping in mind the criticality of infrastructure while at the same time allowing for modern innovations such as the Industrial Internet, standards such as Cyber security Capability Maturity Model (C2M2) has been proposed. C2M2 has three levels of maturity and is publicly available. In particular, C2M2 is made available for the Energy (Electricity) and Oil & Gas sectors. Another effort in this direction is the Cyber Readiness Index, created by M. Hathaway et al and at the

Country level. The v2.0 of this Index was released in November 2015 [7], and it is intended to assess 75 countries using this Index.

The challenge with the Industrial Internet is the retrofitting of sensors to legacy control systems and equipment. Such equipment has not been designed keeping cyber security in mind, and this is of major concern. India has promulgated a National Cyber Security Policy (NCSP) in 2013 and intends to build capacity of half a million cyber security professionals over time to combat such threats.

## II. API ECONOMY

The Amazon internal email from Jeff Bezos in 2003 that exhorted employees to design software with APIs[7], compulsorily, went viral and could be said to be a turning point in the software industry.

In the seminal “IT does not matter” article, Nicholas Carr argued that IT has transitioned from a factor of strategic import to one that is now just a mundane, operational aspect of business [8]. The Corporates have to change their perspective back to the realization that the competitive advantage due to IT in general and software in particular persists. As per the Gartner statement that 75% of the Fortune 1000 will offer Web APIs by 2016, organizations have to revise their view of themselves. For example, Netflix now services nearly 50 million transactions per month [9] through its APIs. Indeed, it is a testimony to how the metadata itself may be more valuable than the transaction data. For example, Netflix API users may be interested to know which are the top 10 movies that are rented in a particular year or to find out which films in languages other than English were most viewed in the past three years.

There was even a more thought provoking blog that proposed that middle managers were being replaced by APIs. There could be some validity to this statement, as aggregators such as Uber function almost entirely by SMS contact - using the Twilio APIs – to communicate with their cab driver/owners.
Even for organizations with a century-old history – such as GE – the API economy is proving to be important. As their customers move from an investment cycle to one of pay as you go (as a service), loss of revenue from sale of assets will necessarily force them to shift to a business model of providing services. Services using the Industrial Internet of Things (GE’s term for IoT) will be provided to their customers to help them prolong the life of their assets. One example would be that of an aircraft, for which sensors are mounted on the wings and other moving parts. Predix operates on top of the sensor infrastructure to derive meaningful information from the terabytes of data collected. It is reported that a single flight from London to New York generates terabytes of data, which needs to be analyzed. This is where Predix (which is Cloud-based) plays a key role. Fuel efficiency, wearing out of aircraft parts are some of the aspects which can be monitored, and actionable information provided to the GE customer.

According to a March 2015 Deloitte report [10], public APIs have doubled in the past 18 months and more than 10,000 APIs have been published to date. Media has been quick to catch on to the provision of APIs, through which their news can be broadcast. Looking at the pervasive use of APIs in sectors as varied as Media, Financial services, Telecom, Energy and Oil & Gas, it can be said that this is the dawn of the API economy. Companies are looking to formulate an API Strategy, and the topic of APIs has moved from being of interest only to developers to the Board Room.

In many cases, cyber security is an afterthought in API design. However, this should not be the case. Even in situations where APIs have not been published publicly, there is always the danger of a disgruntled ex-employee using internal APIs to play havoc. It is reported that organizations in the Financial Services sector spend on average $20 million on controlling cyber security issues. Cyber security insurance has also been offered of late to organization to limit their risk exposure.

## III. APIS AND CYBER SECURITY

We discuss two Indian scenarios where open APIs have been extensively used by the respective industries. First one is Aadhaar - being the flagship project of Government of India and other one YES bank - private player in the market.

### *A. Aadhaar – Unique Identification Authority of India*

The Unique Identification Authority of India (UIDAI) is a central government agency of India. It is attached to NITI Aayog. UIDAI collects biometric and demographic data of residents and stores them in a centralised database. The authority issues a 12-digit unique number called Aadhaar to each resident. Since its inception in the year 2009, it has been a proof of identity and address for various government services such as obtaining new passports, mobile numbers, opening bank accounts etc. Several companies in the private sector use Aadhaar’s biometrics for their attendance. Out of the total one billion mandated enrolment by next year, 700 million residents of India already possess an Aadhaar card.

Three Aadhaar enabled services – an authentication services using Iris, an authentication service using one time pin and an electronic Know Your Customer (eKYC) service has been launched by UIDAI. With this service, UIDAI shares all demographic information including name, address, Date of Birth, Gender, photograph and mobile number to the service providers. Access to such information not only brings up privacy issues but also security concerns. This information is being retrieved even by private players indicates that UIDAI provides an API access to them and this might lead to system abuse. With Iris based authentication service, it is possible to

verify an individual's identity by a combination of Aadhaar number and Iris image through Central Identities Data Repository. One Time Pin authentication is done without biometric verification on a self service mode. Aadhaar enabled service delivery could be linked to various schemes such as Government wage payments, Public Distribution Systems, payment of social security benefits among others.

Aadhaar based hackathon has enabled development of 36 applications that can make use of an individual's unique identification number to smoothly provide several social and economic services. Aadhaar has its own open source API. Developers are encouraged to write codes using API which would benefit many private and public services provided to the end user.

*B. Private player – YES Bank*

Standard & Poor – the credit rating agency - has notified that it could downgrade banks with weak cyber security, even if they have not been attacked. Banks are viewed as 'natural targets facing a high threat of cyber-risk' as they are key nodes in the global financial system. Banks are supposed to equip themselves to prepare for a security attack as their data is very crucial and confidential. For a successful cyber security strategy, banks have to understand when their systems would be maliciously penetrated and must be prepared with necessary actions.

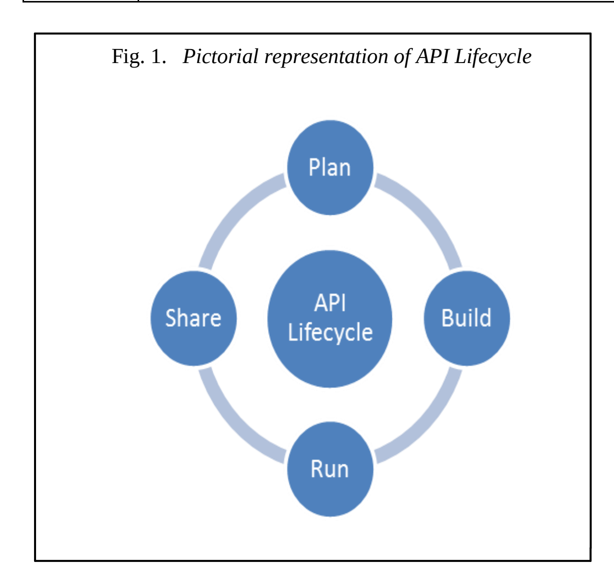
Banks offer variety of services and solutions designated to address different needs of its customers. The current digital banking solutions are fragmented and diverse. Banks are finding it difficult to bring it into a single platform. The digital platform StarKit created by Quantiguous solutions enables banks to quickly deploy diverse applications securely and consistently. This provides a superior experience for consumers while increasing the value of the digital channel for banks. APIs have revolutionized the banking services and their operations. API banking helps banks to overcome challenges in data sharing within the organization. With the API banking platform one can go to a third party's website and shortlist the things where detailed information is required. With minimal effort, the selected bank gets to know the requirement and sends acknowledgement to the user. Yes Bank took a leap of faith and engaged Quantiguous solutions as their partner. The engagement involved reviewing the enterprise architecture, selection and implementation of middle ware stack for the various digital initiatives and building the internal development team.

One of the solutions is when a user's ATM card gets retained in the machine, a phone call to the bank facilitates in solving the challenges faced during this incident. The bank and its managers get the idea of who is calling and for what purpose with all the contact details of the concerned person flashing on their screen at a glance. Thus, open APIs from YES bank have enabled transformation of banking experience with digital banking solutions.

TABLE I. LIFECYCLE OF AN API

| **API Lifecycle** | **Security Issues with APIs** |
|---|---|
| | **External/Public** |
| Plan | Authentication and Authorization |
| Build | Improper coding |
| Run | Off-site data handling, Strength of password, Session length, Concurrent session limitations |
| Share | Launch of dependency versions |

Fig. 1. *Pictorial representation of API Lifecycle*




*Plan:*
At the planning or designing stage, it is important to develop an internal culture of security catering to wide range of solutions and responsibilities. The designer of API must ensure there is not a case of improper session handling encouraging massive security breach. Improper authentication and authorization leads to massive security breaches. Thus exposure of credentials of the administrator puts the data at risk.

*Build:*
Poor error handling, value checking, memory overflow prevention makes the system highly vulnerable. The code which is written might be useful for functionality but not for security purpose. New set of developers who are used to working in legacy systems might make current systems vulnerable by exposing them to cloud solutions with weak authentication. While building APIs it is essential to document the entire procedure to enable the debugging process to be quicker.

To identify potential threats and vulnerabilities threat modelling is taken up at the design stage to counter threats. Here, documentation of the assessed probability of threats with possible counter measures to mitigate the threat is taken up. It is possible that the mitigation takes the form of changing the design itself. Graphical tools are available which would analyze threats, captures impact assessments and their proposed mitigation plans.

*Run:*
The world of API is highly dynamic and constantly changes frequently leading to modification in API architecture. As it is natural; along with the API security issues also evolve in a similar manner. Innovation in cloud computing solutions churns out massive amounts of data thus creating a need for off-site computing. An environment in which local servers and resources were utilizing an API has become open source. This makes these systems vulnerable to outside hijackers. In the catastrophic security issue, there must be quick incidence response triggered in the deployment stage. Periodic update of authentication and authentication is required for continued use of the systems. As the versions of APIs keep changing there could be system vulnerabilities and the newer versions with better security is not updated.

*Share:*
With the World Wide Web burgeoning there is a need for standardized programs to function to make them compatible with external systems. The change from internal design to dependency-centric design creates dependency vulnerabilities thus causing security concerns. Dependency solutions are inevitable while developing APIs. However, when they are exposed to external environment they become vulnerable to security issues. Lack of effective security encryption might lead to complete exposure of network resources thus betraying the entire eco system.

## V. CONCLUSION AND FUTURE SCOPE

A case for keeping the cyber security aspect in the forefront while crafting an API Strategy has been made in this paper. Organizations would do well to assess themselves using cyber security models and guidelines such as the Cyber security Capability Maturity Model (C2M2).

Although India has promulgated the National Cyber Security Policy 2013 (NCSP-2013), specific attention needs to be paid to cyber security assessment and certification. One assessment model that readily comes to mind is the Cyber readiness Index 2.0. The Index will be used to grade 75 selected nations on seven aspects. A specific goal for India may be to improve its Cyber readiness index each year until it reaches the first 10 or 20 countries at the top in terms of cyber security. The deployment of cyber security trained and certified professionals to grade the Industrial Control Systems and Infrastructure would be a first step. Karnataka is one of the first States in India to come up with a startup facility for Internet of Things. Some of the startups could focus their attention on security hardening of critical infrastructure.

In the Government domain, the Aadhaar ecosystem needs to be buttressed as well. Independent cyber security assessment of the Aadhaar open APIs needs to be made prior to every release of the APIs to its ecosystem. Along with cyber security, an organization’s API strategy should also consider aspects such as rights management, filtering at the query and asset levels, user permissions, and data retention. This could be done by way of legal contracts either on an individual basis with its business partners, or as generic Terms of use for all users of the APIs in the API economy. On the Internet of Things from a consumer perspective as well, legal aspects need to be considered.

## REFERENCES

[1] GE Digital, "How SSE Is Optimizing Equipment Performance," 12 January 2016. [Online]. Available: https://www.youtube.com/watch?v=wVul44pA0yI. [Accessed 14 January 2016].

[2] E. K. U. Jacobsen, "Unique Identification: Inclusion and surveillance in the Indian biometric assemblage”, *Security Dialogue*, vol. 43, no. 5, p. 457–474, 2012.

[3] R. Miller, "ge-predicts-predix-platform-will-generate-6b-in-revenue-this-year," 29 September 2015. [Online]. Available: http://techcrunch.com/2015/09/29/ge-predicts-predix-platform-will-generate-6b-in-revenue-this-year/. [Accessed 14 January 2016].

[4] R. Walters, "Cyber Attacks on U.S. Companies in 2014 - Issue Brief IB4289," The Heritage Foundation, Washington, D.C., 2014.

[5] M. Kelley, "The-Stuxnet-Attack-On-Irans-Nuclear-Plant-Was-Far-More-Dangerous-Than-Previously-Thought," 20 November 2013. [Online]. Available: http://www.businessinsider.in/The-Stuxnet-Attack-On-Irans-Nuclear-Plant-Was-Far-More-Dangerous-Than-Previously-Thought/articleshow/26113763.cms. [Accessed 14 January 2016].

[6] K. Zetter, "german-steel-mill-hack-destruction," 8 January 2015. [Online]. Available: http://www.wired.com/2015/01/german-steel-mill-hack-destruction/. [Accessed 14 January 2016].

[7] "the-secret-to-amazons-success-internal-apis," 12 January 2012. [Online]. Available: http://apievangelist.com/2012/01/12/the-secret-to-amazons-success-internal-apis/. [Accessed 14 January 2016].

[8] N. G. Carr, "IT doesn't matter," *Harvard Business Review*, 2003.

[9] B. I. Thomas Davenport, "Move Beyond Enterprise IT to an API Strategy," Harvard Business Review, 6 August 2013. [Online]. Available: https://hbr.org/2013/08/move-beyond-enterprise-it-to-a. [Accessed 14 January 2016].

[10] "day-0-flash-exploits-versioning-and-the-api-space," [Online]. Available: http://nordicapis.com/day-0-flash-exploits-versioning-and-the-api-space/. [Accessed 14 January 2016].

[11] "your-api-is-vulnerable-if-these-4-risks-arent-mitigated," [Online]. Available: http://nordicapis.com/your-api-is-vulnerable-if-these-4-risks-arent-mitigated/. [Accessed 14 January 2016].

[12] [Online]. Available: https://blog.akana.com/api-lifecycle-management/. [Accessed 14 January 2016].

[13] [Online]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=8091. [Accessed 14 January 2016].